Е. В. Барсукова, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732, 004.722

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ СРЕДСТВАМИ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. В работе проведен сравнительный анализ отечественных систем резервного копирования. Предметом исследования стало развертывание системы резервного копирования в виртуальной облачной инфраструктуре, представляющей модель «инфраструктура как услуга». В результате работы обеспечено безопасное и надежное хранение резервных копий виртуальных машин и контроллеров домена FreeIPA, а также разработаны скрипты для автоматизации процесса.

Ключевые слова: резервирование, облачные сервисы, виртуализация, IaaS, RuBackup.

Введение. Сегодня в каждой третьей российской компании внедрена система резервного копирования, занимающая стратегически важное место в обеспечении непрерывности рабочего процесса. Одной из главных задач резервирования является защита от рисков информационной безопасности (далее — ИБ), например, кибератак и повреждений [1]. В связи со сложившейся санкционной политикой иностранных государств, предприятия вынуждены переходить на отечественное программное обеспечение (далее — ПО). Сущность проблемы организации безопасной системы резервного копирования (далее — СРК) сводится к масштабируемости и длительности развертывания. Например, каждому последующему дифференциальному резервированию необходимо больше времени по сравнению с предыдущим [2]. Безопасность играет немаловажную роль в хранении и передаче резервных копий по сети. Хорошим примером угрозы ИБ служит вирус-шифровальщик "WannaCry", который проникает на компьютер, шифрует его, затем сканирует остальные сетевые устройства на наличие необходимой уязвимости и делает с ними то же самое [3].

Следовательно, проблему автоматизации и обеспечения безопасности резервирования важных компонентов инфраструктуры необходимо решать, базируясь на выборе лучшего программного решения [4, 5].

Проблема исследования. Организация безопасного резервного копирования представляет собой выполнение комплекса задач:

- провести сравнительно-сопоставительный анализ функциональных возможностей ПО в области ИБ;
- смоделировать топологию компьютерной сети;
- апробировать выбранный продукт на виртуальной облачной инфраструктуре;
- разработать перечень скриптов, автоматизирующих процесс конфигурации.

Материалы и методы. Методами исследования являются анализ, изучение, моделирование. Виртуальный бэкап-сервер с характеристиками: ОЗУ 4 ГБ, HDD на 50 ГБ, 4-ядерный виртуальный процессор.

Результаты. Для настройки СРК предоставлено виртуальное облако, развернутое с помощью средства виртуализации «Брест» и предоставляющее инфраструктуру как сервис (Infrastructure as a Service, IaaS), при котором организация получает возможность работать с виртуальной инфраструктурой, самостоятельно управляя ее ресурсами, операционными

системами (далее — ОС) и приложениями. Если виртуальная машина выйдет из строя, резервное копирование быстро восстановит ее работу без потери данных.

Одним из ключевых результатов исследования является проведение сравнительно-сопоставительного анализа четырех основных продуктов резервирования: Кибер Бэкап, RuBackup, Rsync и Bacula.

Сравнение проводилось по восьми критериям, из которых первым по значимости стало применение защитных преобразований для предотвращения потерь и кражи резервных копий при их переносе и хранении. Кибер Бэкап, Rsync и Bacula используют алгоритм шифрования AES, который выполняется в режиме цепочки шифрблоков с максимальной длиной ключа 256 бит. Помимо него в функционале RuBackup предоставляется на выбор еще 13 алгоритмов, включая Serpent и Twofish, которые вошли в тройку финалистов конкурса AES. Такое разнообразие позволяет выбирать наиболее подходящий метод в зависимости от политики безопасности компании, что повышает уровень защиты данных. К тому же, Кибер Бэкап не поддерживает и не отвечает за работу OpenSSL, в отличие от RuBackup, который применяет хэш-функцию для цифровой подписи в соответствии с OpenSSL. Поэтому следующим не менее важным критерием стала поддержка электронной подписи асимметричным шифрованием. Резервная копия подписывается цифровой подписью на стороне клиента с целью сопоставления размера файлов копии и самой резервной копии для дальнейшего контроля и предотвращения угрозы ее подмены.

Управление информацией и событиями безопасности (далее — SIEM) есть только у RuBackup, оно осуществляется через консольную утилиту, включающую сбор данных, информирование о состоянии системы, отображение списка событий и экспортирование журнала.

Наличие кластера высокой доступности играет немаловажную роль в случае отказа основного сервера, тогда все запросы будут автоматически перенаправлены на резервный, что поддержит непрерывное обслуживание. А в случае отказа резервного сервера копии могут быть перенаправлены в другое хранилище.

Совокупность вышеперечисленных требований сподвигла сделать выбор в пользу RuBackup, дополнением к этому является его бесшовная совместимость с программным комплексом виртуализации Брест, в отличие от остальных решений. Сравнительная таблица популярных систем резервного копирования изображена на рис. 1.

Критерии сравнения	**Кибер Бэкап**	**Рубэкап**	**Rsync**	**Bacula**
SIEM	-	rb_security	-	-
Модель доступа	Ролевая	Ролевая	-	-
Отказоустойчивость	+	+	-	-
Электронная подпись	-	+	-	+
Защитное преобразование	+	+	+	+
Приоритеты задач резервирования	-	+	-	-
Централизованное восстановление	+	+	-	+
Совместимость со средством виртуализации "Брест"	+	+	+	+

Рис. 1. Сравнение систем резервного копирования

Существует известный принцип резервного копирования «3-2-1». Предполагается создание трех копий, одна из которых хранится в облаке, а еще две — на отдельных друг от друга физических носителях, что делает данные, хранящиеся на трех бэкапах, практически нерушимыми. Эта система была учтена и реализована в проектируемой СРК облачной инфраструктуры.

С целью автоматизировать и ускорить процесс организации резервирования был разработан перечень скриптов.

- Базовая настройка ОС, сетевых интерфейсов и SSH (Bash).
- Установка клиентов на сервера «Брест» и FreeIPA (Ansible).
- Создание сервера RuBackup (Ansible).
- Добавление резервного сервера RuBackup (Ansible).
- Обновление пакетов серверов (Ansible).
- Удаление клиента и сервера (Ansible).

В результате работы скриптов были организованы виртуальные серверы резервного копирования, внедренные в облачную инфраструктуру, развернуты клиенты на серверах виртуализации для дальнейшего резервирования виртуальных машин (рис. 2).

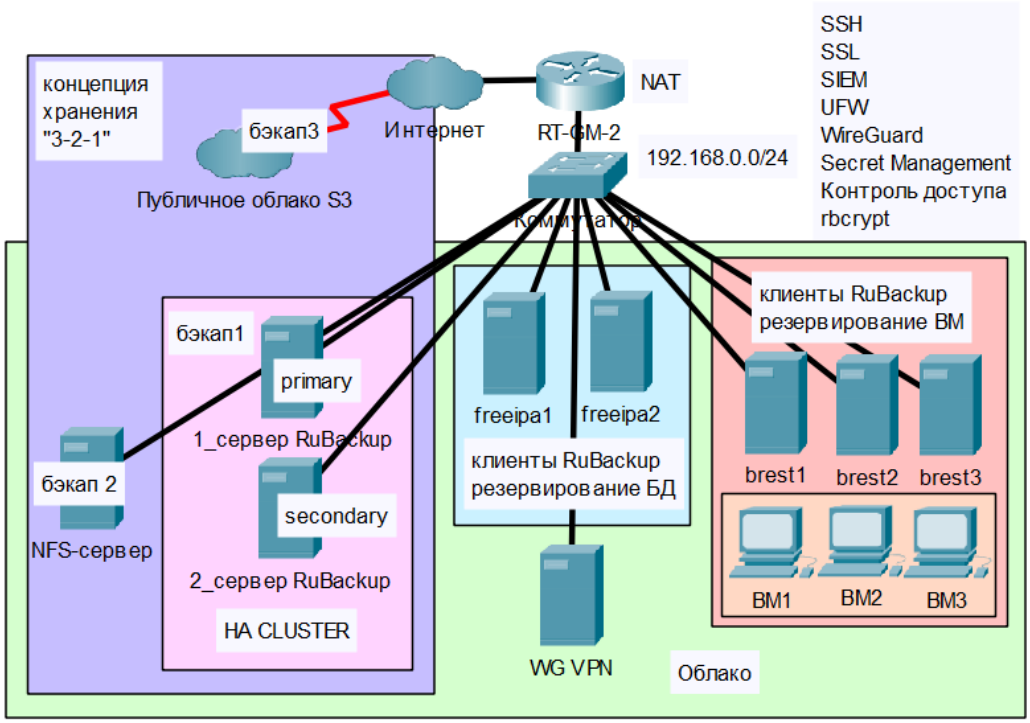

Рис. 2. Топология сети

Развертывание всей СРК вручную занимает приблизительно 7 часов с учетом всех погрешностей. Со скриптами, разработанными в ходе работы, можно ускорить настройку конфигурации в 1,5 раза, что соответствует 4,5 часам. Так, например, Ansible-скрипт по установке клиентов СРК на сервера «Брест» и FreeIPA содержит в себе:

- обновление операционной системы хоста;
- установку компрессоров, функции использования NFS-папки, библиотек, пакета клиента "RuBackup";

– первоначальную настройку клиента: добавление пользователя в группу, настройка среды для пользователя и перезагрузка;

– включение сервиса клиента, перезагрузка службы, запуск сервиса rubackup_client.

Заключение. Таким образом, проведенный сравнительный анализ отечественных систем резервирования, выявленные особенности стека технологий, моделирование компьютерной сети, позволили организовать безопасное автоматическое резервное копирование в облачной инфраструктуре средствами отечественного программного обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. Айкашева Ю.А. Резервное копирование и восстановление данных на предприятиях / Ю.А. Айкашева // Актуальные проблемы авиации и космонавтики: Учредители: Сибирский государственный университет науки и технологий им. акад. М.Ф. Решетнева, 2016. — С. 7-8. — EDN XRYARX. — URL: https://www.elibrary.ru/download/elibrary_28146253_43682382.pdf (дата обращения: 27.03.2024).
2. Кузнецов И.А. Автоматизация создания резервной копии данных / И.А. Кузнецов // Социально-экономические и технические проблемы оборонно-промышленного комплекса России: история, реальность, инновации: Издательство: Нижегородский государственный технический университет им. Р.Е. Алексеева, Нижний Новгород, 2023. — С. 318-324. — EDN NAEUHL. — URL: https://www.elibrary.ru/download/elibrary_53823738_98958718.pdf (дата обращения: 28.03.2024).
3. Матющенко И.А. Защита и резервация данных системы / И.А. Матющенко, В.М. Енин // Большая студенческая конференция: Издательство «Наука и Просвещение» (ИП Гуляев Г.Ю.), Пенза, 2023. — С. 84-87. — EDN YMIBZW. URL: https://www.elibrary.ru/download/elibrary_53697215_79837014.pdf (дата обращения: 11.04.2024).
4. Щепетова Е.Д. Сетевая автоматизация / Е.Д. Щепетова, С.В. Малахов // Вопросы устойчивого развития общества: Учредители: ООО «Институт развития образования и консалтинга», 2022. — С. 1473-1476. — EDN DBMVDV. URL: https://www.elibrary.ru/download/elibrary_48441813_12025277.pdf (дата обращения: 20.03.2024).
5. Марченко В.С. Анализ реализации стандартной организации защиты информации на предприятии / В.С. Марченко // Вестник Поволжского государственного университета сервиса. Серия: Экономика: Учредители: Поволжский государственный университет сервиса, 2016. — С. 209-213. — EDN VSNWVJ. — URL: https://www.elibrary.ru/download/elibrary_25797838_67708108.pdf (дата обращения: 28.04.2024).